Release Notes

Version 07.8.01d Operating System

for the ProCurve 9304M, 9308M, and 9315M Routing Switches
with Redundant Management (M2, M4, EP, and T-Flow), March 2006

Software release 07.8.01d supersedes earlier software releases in the 07.*x* software branch. (For information about software branches and minimum release requirements for management module support, refer to “Software Branches” on page 3.)

The 07.8.01d release notes provide information on the following items:

- New hardware and software enhancements introduced with software release 07.8.01d
- Known issues in software release 07.8.01d
- Procedure for upgrading the software code on ProCurve 9304M, 9308M, and 9315M Routing Switches with M2, M4, or EP Redundant Management modules. See “Upgrading Software on an M2, M4, or EP Management Module to Release 07.8.01d” on page 7.
- General procedures, usage information, and helpful notes for operating and managing ProCurve routing switches
- Software fixes in release 07.8.01d and earlier releases

Descriptions of the enhancements in release 07.8.00 are included in the manuals for the 07.8.00 release. If you purchased a Redundant Management module with software version 07.8.00 or greater installed, the CD shipped with the module includes the 07.8.00 manuals.

If you need to access ProCurve product documentation, refer to “Downloading the Latest Software and Documentation” on page 3 for information on how to download PDF versions of the latest manuals.

NOTES:

Software Update Notice: Check the ProCurve Website frequently for free software updates for various ProCurve switch products. (Refer to “Downloading the Latest Software and Documentation” on page 3.)

Mini-GBIC ports: Hewlett-Packard offers and supports only mini-GBICs having a ProCurve label (with product number J4858B, J4859B, or J4860B) for use with the following modules:
- J4856A ProCurve 9300 Mini-GBIC Module
- J4857A ProCurve 9300 Mini-GBIC Redundant Management Module
- J4885A ProCurve 9300 EP 8-port Mini-GBIC Redundant Management Module
- J4894A ProCurve 9300 EP 16-port Mini-GBIC Module
- J8177B ProCurve Gigabit-copper mini-GBIC is supported for use in only the EP modules (J4885A and J4894A)

Use of other brands of mini-GBICs is not supported.

Flash Images: The flash image files for this software release differ depending on the type of management module you use. Refer to “Boot Code Requirements for ProCurve Software” on page 5.

SNMP: Starting with software release 05.2.16, the software does not have a default read-write SNMP community. If you use the default community name “private” as the password for web management access or for read-write access through a network management application, you need to use the CLI to add the read-write community string first.

Devices Without Redundant Management: For information about how to upgrade software on the ProCurve 9304M and ProCurve 9308M routing switches without redundant management, refer to the latest 6.6.*x* release notes. (See “Downloading the Latest Software and Documentation” on page 3.)

Publication Number

5991-4722
March 2006

Applicable ProCurve 9300 (Current) Products

9304M Routing Switch . . . . . (J4139A)
9308M Routing Switch . . . . . (J4138A)
9315M Routing Switch . . . . . (J4874A)

EP 10/100-TX RJ-45 Module . . . . . (J4881B)
EP 10/100-TX Telco (RJ-21) Module . . . . . (J4889B)
EP Mini-GBIC RM Module . . . . . (J4885A)
EP Mini-GBIC Module. . . . . (J4894A)
EP 100/1000-T Module. . . . . (J4895A)
2-Port 10 Gigabit Ethernet Module . . . . . (J8174A)
EP 100Base-FX Module . . . . . (J8178A)

Gigabit-SX-LC Mini-GBIC . . . . . (J4858B)
Gigabit-LX-LC Mini-GBIC . . . . . (J4859B)
Gigabit-LH-LC Mini-GBIC . . . . . (J4860B)
1000Base-T Mini-GBIC. . . . . (J8177B)

10 Gigabit Ethernet LR Optic . . . . . (J8173A)
10 Gigabit Ethernet SR Optic . . . . . (J8175A)
10 Gigabit Ethernet ER Optic . . . . . (J8176A)

9304M/9308M Redundant Power Supply. . . . (J4147A)
9315M Redundant Power Supply. . . . . (J4875A)

Trademark Credits

Microsoft®, Windows®, and Windows NT® are trademarks of Microsoft Corporation. Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated. SuperSpan® is a trademark of Foundry Networks, Inc.

Disclaimer

The information contained in this document is subject to change without notice.

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Warranty

See the Customer Support/Warranty booklet included with the product.

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.

Hewlett-Packard Company
8000 Foothills Blvd.
Roseville, CA 95747-5551
USA
http://www.procurve.com

Contents

Terminology

The following table defines basic product terms used in ProCurve routing switch documentation.

Term	Definition
chassis device or chassis	A routing switch that accepts optional modules or power supplies. The ProCurve 9315M, ProCurve 9304M, and ProCurve 9308M routing switches are chassis devices.
EP (Enhanced Performance) and Standard	Routing switches can be EP or Standard devices, depending on whether the management module is an EP or Standard (M2 or M4) module. For a listing of ProCurve routing switches and their product numbers, see Table 4 on page 5.
routing switch or router	A Layer 3 device that switches and routes network traffic. The term *router* is sometimes used in this document in descriptions of a routing switch's Layer 3 routing protocol features.
switch	A Layer 2 device that switches network traffic.
`ProCurve 9300#`	An example Command Line Interface (CLI) prompt. Actual prompts show the product number for the routing switch, such as ProCurve 9300#.

Product Documentation for Software Release 07.8.01d

Software release 07.8.01d includes all of the features in release 07.8.00a, plus several new features.

- For documentation on the features in 07.8.01d that were available in earlier releases, refer to the product documentation set identified for "Software Version 07.8.00a".

Table 1 describes the main topics covered in the ProCurve Routing Switch documentation set. If you do not already have a PDF version of the 07.8.00a documentation set, refer to "Downloading the Latest Software and Documentation" on page 3.

Table 1: Where To Get More Information

Title	Contents

Installation and Basic Configuration Guide	• Installation
	• Basic Features
	  • System (SNMP, SNTP, Syslog, broadcast and multicast throttling)
	  • Port configuration (speed, mode)
	  • Layer 2 (MAC table parameters, MAC filters, broadcast and multicast filters, port locks)
	  • Parameter table resizing
	  • Port monitoring
	• Link Aggregation
	• Spanning Tree Protocol
	• Virtual LANs
	• Layer 2 Multicast
	• Base Layer 3
	• Upgrading Software (**Important:** See also "Upgrading Software on an M2, M4, or EP Management Module to Release 07.8.01d" on page 7 in this document.)
	• Hardware Specifications and RFCs

Security Guide	• Security (passwords, user accounts, AAA, RADIUS, and TACACS/TACACS+) • Secure Shell (SSH) • Denial of Service Protection
Advanced Configuration and Management Guide	• QoS • ACLs • EP rate limiting • Standard rate limiting • IP • RIP • IP Multicast • OSPF • BGP4 • Network Address Translation • VRRP and VRRPE • IPX • AppleTalk
Command Line Interface Reference	Syntax information for all CLI commands.
Diagnostics Guide	• Diagnostic commands • Backplane debugging commands • Changing CAM partitions

Downloading the Latest Software and Documentation

You can download software version 07.8.01d and the latest routing switch product documentation from the ProCurve website as described below.

To Download a Software Version:

1. Go to the ProCurve website at **http://www.procurve.com**.
2. Click on **software** (in the sidebar).
3. Under “latest software”, click on **switches**.

NOTE: If you are downloading software for the ProCurve 9304M or ProCurve 9308M, select the option that matches the type of management module(s) you are using in the routing switch—with redundant management or without redundant management.

To Download Product Documentation:

For the latest version of product documentation for ProCurve routing switches:

1. Go to the ProCurve website at **http://www.procurve.com**.
2. Click on **technical support**, then **manuals**.
3. Click on the name of the product for which you want manuals.
4. On the page listing the manuals, find the latest manuals under the heading “**For software version 7.8.00a**”.

You will need the Adobe® Acrobat® Reader (version 4.0 or greater) to view or print the manuals.

Software Branches

Starting with software releases 06.6.28 and 07.1.10, ProCurve offers the software branches described in Table 2:

Table 2: Software Branches

Software Release	Includes:	Operates on:
06.6.28 and later 06.*x* releases	Bug fixes	ProCurve 9304M and ProCurve 9308M routing switches without redundant management (that is, with M1 modules) ProCurve 6308M-SX routing switch ProCurve 6208M-SX switch
07.1.10 and later 07.1.x releases	Bug fixes, new features, and enhancements to existing features	ProCurve 9304M and ProCurve 9308M routing switches with redundant management (M2 modules)
07.5.04 release	Bug fixes, new features, and enhancements to existing features	ProCurve 9304M, ProCurve 9308M, and ProCurve 9315M routing switches with redundant management (M2 and M4 modules)
07.6.00 and 07.6.01b releases	Bug fixes, new features, and enhancements to existing features	ProCurve 9304M, ProCurve 9308M, and ProCurve 9315M routing switches with redundant management (M2, M4, EP, and T-Flow) and 1-port 10GB modules
07.6.04 release 07.7.01 release	Bug fixes, new features, and enhancements to existing features, including support for the 2-port 10GB module	ProCurve 9304M, ProCurve 9308M, and ProCurve 9315M routing switches with redundant management (M2, M4, EP, and T-Flow) and 2-port 10GB modules

Table 2: Software Branches

Software Release	Includes:	Operates on:
07.7.01b release	Bug fixes, 07.7.01 features and enhancements to existing features, and a new procedure for upgrading software code	ProCurve 9304M, ProCurve 9308M, and ProCurve 9315M routing switches with redundant management (M2, M4, EP, and T-Flow) and 2-port 10GB modules
07.8.00a release	Bug fixes, new 07.8.00a hardware and software features, and enhancements to existing features	ProCurve 9304M, ProCurve 9308M, and ProCurve 9315M routing switches with redundant management (M2, M4, EP, and T-Flow) and 2-port 10GB modules

Software Requirements for Management Modules

Table 3 shows the minimum software releases required to run redundant management modules.

Table 3: Minimum Software Requirements for Management Modules

Minimum Software Release Required	ProCurve 9300 Series Redundant Management Modules Supported
07.1.10 Supported only on ProCurve 9304M and 9308M	J4845A ProCurve 9300 GigLX Redundant Management Module (8-port, M2) J4846A ProCurve 9300 GigSX Redundant Management Module (8-port, M2) J4847A ProCurve 9300 Redundant Management Module (0-port, M2)
07.1.19 Supported only on ProCurve 9304M and 9308M	All of the redundant management modules supported for release 07.1.10 J4857A ProCurve 9300 Mini-GBIC Redundant Management Module (8-port, M4)
07.5.04 Supported on ProCurve 9304M, 9308M, and 9315M	All of the redundant management modules supported for release 07.1.19 J4879A ProCurve 9300 T-Flow Redundant Management Module
07.6.00 Supported on ProCurve 9304M, 9308M, and 9315M	All of the redundant management modules supported for release 07.5.04 J4885A ProCurve 9300 EP Mini-GBIC Redundant Management Module

Software Supported on ProCurve Routing Switches

Table 4 shows the software releases supported on each ProCurve routing switch.

Table 4: Software Releases Supported on ProCurve Routing Switches

Routing Switch	Software Releases Supported			
	M2 or M4 Redundant Mgmt **H2R05216.BIN** **H2R06605.BIN** **H2R06616.BIN** **H2R07110.BIN** **H2R07119.BIN** **H2R07122.BIN** **H2R07124.BIN**	**M2 or M4 Redundant Mgmt** **H2R07504.BIN[1]** **H2R07600.BIN[2]** **H2R07601.BIN** **H2R07604c.BIN** **H2R07701b.BIN** **H2R07800a.BIN** **H2R07801d.BIN**	**M1 Router Code only** **HPR05216.BIN** **HPR06605.BIN** **HPR06616.BIN** **HPR06628.BIN** **HPR06633.BIN** **HPR06636.BIN**	**M1 Switch Code only** **HPS05216.BIN** **HPS06605.BIN** **HPS06616.BIN** **HPS06628.BIN** **HPS06633.BIN** **HPS06636.BIN**
ProCurve 9315M (J4874A) Routing Switch with EP or Standard (M2 or M4) Redundant Management Module(s)	No	Yes	No	No
ProCurve 9304M (J4139A) and 9308M (J4138A) Routing Switches with EP or Standard (M2 or M4) Redundant Management Module(s)	Yes	Yes	No	No
ProCurve 9304M (J4139A) and 9308M (J4138A) Routing Switches without Redundant Management (with M1 Management Module)	No	No	Yes	No
ProCurve 6308M-SX (J4840A) Routing Switch	No	N/A	Yes	No
ProCurve 6208M-SX (J4841A) Switch	No	N/A	No	Yes

[1]First software release to support the ProCurve 9315M routing switch and the J4879A T-Flow module

[2]First software release to support the EP (Enhanced Performance) modules.

Boot Code Requirements for ProCurve Software

To run a software release on a ProCurve routing switch, you must use the minimum version of boot code for each software image described in Table 5.

Table 5: Boot Code Requirements

Routing Switch	Modules	Software Image	Minimum Boot Code Required
ProCurve 9304M ProCurve 9308M	With one of the following M1[1] modules (without Redundant Management): J4141A 10/100 J4144A Gigabit SX J4146A Gigabit 4LX/4SX	HPR06636.bin[2]	M1B07108.bin or greater recommended
ProCurve 9304M ProCurve 9308M ProCurve 9315M	With any one or two of the following Redundant Management: modules J4846A Gigabit SX[2] (M2) J4845A Gigabit LX[2] (M2) J4847A 0-Port[2] (M2) J4857A Mini-GBIC (M4) J4885A EP J4879A T-Flow	For M2, M4, and EP Redundant Management modules: - H2R07801d.bin For T-Flow Redundant Management modules: - TSP07801d.bin	For M2, M4, and EP Redundant Management modules: - M2B07605.bin or greater For T-Flow Redundant Management modules: - M2B07605.bin (all MP images) - VSB07100.bin (VSM code)
—	10 Gigabit Ethernet (10GE) Modules **Note:** To upgrade FPGA code, refer to “Upgrading the FPGA on a 10 Gigabit Ethernet Module” on page 11.	The Field-Programmable Gate Arrays (FPGAs) in 10 Gigabit Ethernet Modules use the following software. J4891A FPGA: rxbmgr.bin – version 80, revision 6 rxpp.bin – version 81, revision 16 txaccum.bin – version 82, revision 6 txpp.bin – version 83, revision 13 ageram.bin – version 84, revision 4 J8174A FPGA: xpp.bin – version 88, revision 37 xtm.bin – version 89, revision 39 **Note**: To determine the FPGA versions running on a 10GE module, enter **show flash**. The version information is listed separately for each 10 Gigabit Ethernet module in the chassis.	10 Gigabit Ethernet modules do not use any of the boot images listed above.
ProCurve 6308M-SX	—	HPR06636.bin[2]	M1B07108.bin or greater recommended

Routing Switch	Modules	Software Image	Minimum Boot Code Required
ProCurve 6208M-SX	—	HPS06636.bin[2]	M1B07108.bin or greater recommended

[1]M1 management modules (without Redundant Management) have been discontinued.

[2]Does not support Secure Shell (SSH) version 1.

Upgrading Software on an M2, M4, or EP Management Module to Release 07.8.01d

This section explains how to upgrade the software used on M2, M4, and EP redundant management modules on a ProCurve 9304M, ProCurve 9308M, or ProCurve 9315M routing switch to release 07.8.01d.

NOTE: As shown in Table 5, newer software versions require newer versions of boot code. Software versions use a five-digit number in the format: xx.x.xx; for example, 07.8.01d. Boot code versions use a six-digit number in the format: xx.xx.xx; for example, 07.06.05.

Different procedures are used to upgrade an M2, M4, or EP management module, depending on the version of software running on the module:

- A software release earlier than 07.6.01b
- Software release 07.6.01b or greater

NOTE: M1 Management modules (discontinued) do not support software releases 07.x.xx, and are, therefore, not described in this section. The latest software release supported on an M1 management module is 06.6.36.

Restrictions

- Software release 07.8.01d requires boot code version 07.06.05 to support all hardware modules and decompress new software images.

  A new compression algorithm was introduced in software releases greater than 07.6.01b to generate software images. The new compression algorithm allows a software image to contain more features.

  Software release 07.6.01b was introduced as a special release that is used as an intermediate step when you upgrade to a later software release. After you install release 07.6.01b and reboot a routing switch, the switch is able to copy the latest software images to flash memory.

- On an M2, M4, or EP redundant management module, boot code is not automatically copied from the active to the standby management module. (However, software code is automatically copied to a standby management module.)

  To copy boot code from the active to a standby management module, you must enter the **sync boot** command.

- On a ProCurve 9315M, software release 07.5.04 is the earliest release supported. If a management module is running software earlier than release 07.5.04, you cannot upgrade the module in a 9315M chassis. Instead, you must upgrade it in a 9304M or 9308M chassis.

Upgrading to Software Release 07.8.01d: Overview

To upgrade an M2, M4, or EP management module to release 07.8.01d, you must follow these general steps:

A. Upgrade the boot code on the management module to version 07.06.05. If necessary, use the **sync boot** command to copy boot code from the active to a standby management module in the routing switch. Then reboot the routing switch to load boot code 07.06.05.

B. If the routing switch is running software EARLIER than release 07.6.01b, copy release 07.6.01b to flash memory. Then reboot the device to load the 07.6.01b software.

C. Copy release 07.8.01d to flash memory, and reboot the routing switch to load 07.8.01d software.

A. Upgrading Boot Code on a Management Module to Version 07.06.05

To upgrade the boot code on an M2, M4, or EP management module to version 07.06.05:

1. Store boot code version 07.06.05 (filename: M2B07605.bin) on a TFTP server that the routing switch can access.
2. Enter the following command at the privileged EXEC level of the CLI (for example: ProCurve 9300#) to copy the boot code from the TFTP server into the flash memory of the management module:

   copy tftp flash <*ip-addr*> <*image-file-name*> **boot**
3. Verify that the code has been successfully copied by entering the following command at any level of the CLI:

   show flash

   The boot code version is displayed on the line that begins with “Boot Image size”. Ensure that boot code version 07.06.05 is displayed for the active management module.
4. If a standby (redundant) management module is installed in the routing switch, synchronize the boot code on the standby management module by entering the **sync boot** command.

   Verify that boot code 07.06.05 has been successfully copied on the standby management module by entering the **show flash** command.
5. Reboot the routing switch to load boot code 07.06.05.

B. Upgrading Software on a Management Module From a Release Earlier than 07.6.01b

To upgrade the software on an M2, M4, or EP management module from a release EARLIER than 07.6.01b to release 07.8.01d:

1. Verify the version of boot code installed on the management module by entering the **show flash** command.

   The boot code version is displayed at the end of the line that begins with “Boot Image size”. Ensure that boot code version 07.06.05 is displayed.

   NOTE: The **show flash** command only displays the version of boot code installed on the device. It does not display the version of boot code running on the device.

   If you rebooted the routing switch after installing boot code 07.06.05 (as described in “A. Upgrading Boot Code on a Management Module to Version 07.06.05”), the required boot code is running. If you are not sure, ProCurve recommends that you reboot the device now.

   ---
2. Store software release 07.6.01b (filename: H2R07601b.bin) on a TFTP server that the routing switch can access.
3. Upgrade the software on the management module to version 07.6.01b by entering the following command:

   copy tftp flash <*ip-address*> **H2R07601b.bin** [**primary | secondary**]

   Where:

   primary copies software to the primary (default) storage area in flash memory.

   secondary copies software to the secondary area in flash memory.

   If no redundant management module is installed, the message `TFTP to Flash Done` is displayed when the upgrade is complete.

   If a redundant management module is installed, the message `Sync Secondary code in flash...Done`

is displayed when the flash images are synchronized and the upgrade is complete.

4. Verify that the software has been successfully copied by entering the **show flash** command at any level of the CLI:
   - The software release in the primary flash is displayed at the end of the line that begins with “Compressed Pri Code Size”.
   - The software release in the secondary flash is displayed at the end of the line that begins with “Compressed Sec Code Size”.

   Ensure that software release 07.6.01b is stored in the primary or secondary flash area.
5. Reboot the routing switch to load software release 07.6.01b from the area of flash memory (primary or secondary) where you stored it.
6. Continue with “C. Upgrading Software on a Management Module From Release 07.6.01b or Greater” to upgrade the software to release 07.8.01d.

C. Upgrading Software on a Management Module From Release 07.6.01b or Greater

To upgrade the software on an M2, M4, or EP management module from release 07.6.01b or greater to release 07.8.01d:

1. Verify the version of boot code running on the management module by entering the **show flash** command.

   The boot code version is displayed at the end of the line that begins with “Boot Image size”. Ensure that boot code version 07.06.05 is displayed.

   NOTE: The **show flash** command only displays the version of boot code installed on the device. It does not display the version of boot code running on the device.

   If you rebooted the routing switch after installing boot code 07.06.05 (as described in “A. Upgrading Boot Code on a Management Module to Version 07.06.05”), the required boot code is running. If you are not sure, ProCurve recommends that you reboot the device now.

   ---
2. Store software release 07.8.01d (filename: H2R07801d.bin) on a TFTP server that the routing switch can access.
3. Upgrade the software on the management module to version 07.8.01d by entering the following command:

   copy tftp flash <*ip-address*> **H2R07801d.bin** [**primary | secondary**]

   Where:

   primary copies software to the primary (default) storage area in flash memory.

   secondary copies software to the secondary storage area.

   If no redundant management module is installed, the message `TFTP to Flash Done` is displayed when the upgrade is complete.

   If a redundant management module is installed, the message `Sync Secondary code in flash...Done` is displayed when the flash images are synchronized and the upgrade is complete.
4. Verify that the software has been successfully copied by entering the **show flash** command at any level of the CLI:
   - The software release in the primary flash is displayed at the end of the line that begins with “Compressed Pri Code Size”.
   - The software release in the secondary flash is displayed at the end of the line that begins with “Compressed Sec Code Size”.

   Ensure that software release 07.8.01d is stored in the primary or secondary flash area.

5. Reboot the routing switch to load software release 07.8.01d from the area of flash memory (primary or secondary) where you stored it.

NOTE: When you reload the software after upgrading the software to release 07.8.01d, the routing switch displays a message to say that the configuration has changed and prompts you to save the changes. This message is displayed even if you do not make any configuration changes because the software records its release number in the running-config file when the software is loaded onto the switch. Enter **Y** to reload without saving the change or save the change and reload.

Using SNMP to Upgrade Software on a Management Module

Third-party SNMP management applications such as HP OpenView can upgrade software on a routing switch.

NOTE: In software releases earlier than 07.5.04, the SNMP agent does not check for type validity with the SNMP version. In software release 07.5.04 and greater, the SNMP agent does not send a reply for a varbind, if the type of the varbind is not a known type for that version of SNMP. For example, MIB objects of type Counter64 cannot be retrieved using a v1 packet, as Counter64 is a v2c and v3 type.

Make sure you use the correct procedure for your device and processor type. For example, do not use the Management Processor procedure to upgrade the switching processors on a T-Flow module.

The syntax shown in this section assumes that you have installed HP OpenView in the “/usr” directory.

ProCurve recommends that you make a backup copy of the startup-config file before you upgrade the software. If you need to run an older release, you will need to use the backup copy of the startup-config file.

Upgrading a Management Processor using SNMP

Use the following procedure to upgrade:

- An M2, M4, or EP module
- Management processor on the T-Flow module

To upgrade software code on the Management Processor:

1. Configure a read-write community string on the ProCurve device, if one is not already configured. To configure a read-write community string, enter the following command from the global CONFIG level of the CLI:

   snmp-server community <*string*> **rw**

   where <*string*> is the community string and can be up to 32 characters long.

2. On the ProCurve device, enter the following command from the global CONFIG level of the CLI:

   no snmp-server pw-check

   This command disables password checking for SNMP set requests. If a third-party SNMP management application does not add a password to the password field when it sends SNMP set requests to an ProCurve device, by default the ProCurve device rejects the request.

3. From the command prompt in the UNIX shell, enter the following command:

   /usr/OV/bin/snmpset -c <*rw-community-string*> <*hp-ip-addr*> **1.3.6.1.4.1.1991.1.1.2.1.5.0 ipaddress** <*tftp-ip-addr*> **1.3.6.1.4.1.1991.1.1.2.1.6.0 octetstringascii** <*file-name*> **1.3.6.1.4.1.1991.1.1.2.1.7.0 integer** <*command-integer*>

   Where:
   <*rw-community-string*> is a read-write community string configured on the ProCurve device.
   <*hp-ip-addr*> is the ProCurve device’s IP address.

<*tftp-ip-addr*> is the TFTP server's IP address.
<*file-name*> is the image file name.
<*command-integer*> is one of the following values:
20 – Downloads the software code into the device's primary flash area.
22 – Downloads the software code into the device's secondary flash area.

Upgrading the FPGA on a 10 Gigabit Ethernet Module

This section explains how to upgrade an FPGA (Field-Programmable Gate Array) on a 10 Gigabit Ethernet module. 10 Gigabit Ethernet modules do not have boot code separate from the management module. However, they do have FPGAs that require separate software.

NOTE: The J8174A 2-port 10 Gigabit Ethernet module with XENPAK optics uses a different FPGA file than the older J4891A 1-port 10 Gigabit Ethernet module. See Table 5 on page 6 for a list of the FPGA files supported on both the 1-port and 2-port 10 Gigabit Ethernet modules.

The J8174A 2-port 10 Gigabit Ethernet module with XENPAK optics can function in the same chassis with the older J4891A 1-port 10 Gigabit Ethernet module.

If an upgrade is required for any of the FPGA files, you must upgrade all the FPGA files.

To upgrade the FPGA on a 10 Gigabit Ethernet module:

1. Complete the upgrades of the boot code and software code, if required.
2. Enter the following command for the 10 Gigabit Ethernet module at the privileged EXEC level of the CLI:

   10gig copy tftp flash <*ip-addr*> <*filename*> [**module** <*slotnum*>]

   Where:

   tftp specifies the location of the FPGA file. The **tftp** parameter shows that the file is on a TFTP server.

   <*ip-addr*> specifies the IP address of the TFTP server, if you specify **tftp**.

   <*filename*> specifies the FPGA file name. The 2-port 10 Gigabit Ethernet module has only two FPGA files; xpp.bin and xtm.bin. For more information on the supported FPGA files, see Table 5 on page 6.

   module <*slotnum*> is an optional parameter that specifies the modules on which you want to install the upgrade. If you do not specify a slot number, the command upgrades the FPGA on all 10 Gigabit Ethernet modules in the chassis.

   Example

   ```
   ProCurve 9300# 10gig copy tftp flash 10.10.10.10 rxbmgr.bin
   ProCurve 9300# 10gig copy tftp flash 10.10.10.10 rxpp.bin
   ProCurve 9300# 10gig copy tftp flash 10.10.10.10 txaccum.bin
   ProCurve 9300# 10gig copy tftp flash 10.10.10.10 txpp.bin
   ProCurve 9300# 10gig copy tftp flash 10.10.10.10 ageram.bin
   ```

   NOTE: You can store and copy the FPGA files using any valid filename. You are not required to store and copy the files using the names listed in "Boot Code Requirements for ProCurve Software" on page 5. The device uses information within the files to install them in the correct FPGAs, and the **show flash** command lists the FPGAs according to the names in "Boot Code Requirements for ProCurve Software" on page 5.

   ---

3. Reload the software by entering one of the following commands:
   - **reload** (this command boots from the default boot source, which is the primary flash area by default)
   - **boot system flash primary | secondary**

NOTE: The **show flash** command will list the new FPGA code versions but the new versions do not take effect until you reload the software.

Using Different Combinations of Management Modules

This section describes the different combinations of M1, M2, M4, EP, and T-Flow management modules supported on ProCurve 9304M, ProCurve 9308M, and ProCurve 9315M routing switches.

Table 6: Supported Management Module Combinations

Primary Management Module	Secondary Management Module	Notes
J4885A EP Mini-GBIC Redundant Management Module	Another EP Redundant Management Module	—
Any M2 or M4 Redundant Management Module (*Discontinued*)	Another M2 or M4 Redundant Management Module	When you use an M2 and M4 in the same switch, ProCurve recommends using the faster M4 as the primary redundant management module. If the M4 fails, the system will use the slower M2 module.
J4879A T-Flow Redundant Management Module (*Discontinued*)	Another J4879A T-Flow Redundant Management Module	—
Any M1 Management Module (*Discontinued*)	N/A	Supported only in the ProCurve 9304M and ProCurve 9308M routing switches. No redundant management options.

NOTE: The following types of management modules are *mutually exclusive*:
- M1 management modules
- M2 or M4 redundant management modules
- EP redundant management modules
- T-Flow redundant management modules

A ProCurve routing switch does not operate if two redundant management modules of different types are installed. Also, M1 management modules do not operate in a ProCurve 9315M routing switch.

Redundant management means that a device can operate with two management modules installed; one active (primary) and one standby (secondary). If the active management module becomes unavailable, the standby management module automatically takes over system operation.

Management modules with redundant management capabilities include the following M2, M4, EP, and T-Flow modules:

- J4885A ProCurve 9300 EP Mini-GBIC Redundant Management Module (8-port)
- J4879A ProCurve 9300 T-Flow Redundant Management Module (0-port — *discontinued*)
- J4857A ProCurve 9300 Mini-GBIC Redundant Management Module (8-port, M4 — *discontinued*)
- J4845A ProCurve 9300 GigLX Redundant Management Module (8-port, M2 — *discontinued*)
- J4846A ProCurve 9300 GigSX Redundant Management Module (8-port, M2 — *discontinued*)
- J4847A ProCurve 9300 Redundant Management Module (0-port, M2 — *discontinued*)

If you are using a Redundant Management module, you can install either one or two such modules in the routing switch, as shown in Table 6. For more information, see “Using Redundant Management Modules” in the *Installation and Basic Configuration Guide* included on the *Documentation CD-ROM* shipped with your

management module, and also downloadable from the ProCurve website (see “To Download Product Documentation:” on page 3).

Non-Redundant Management on ProCurve 9304M and ProCurve 9308M Routing Switches

Management modules without Redundant Management are sometimes termed “M1” modules (for “Management 1”). These modules, now discontinued, operate only in the ProCurve 9304M and ProCurve 9308M routing switches. M1 modules include:

- J4141A ProCurve 9300 10/100 Management Module (16-port — *discontinued*)
- J4144A ProCurve 9300 Gigabit SX Management Module (8-port — *discontinued*)
- J4146A ProCurve 9300 Gigabit 4LX/4SX Management Module (8-port — *discontinued*)

NOTE: M1 management modules do not operate in the ProCurve 9315M routing switch. Also, if you are using an M1 management module in a ProCurve 9304M or ProCurve 9308M, no other management module (non-redundant or redundant) can be installed in the routing switch.

Maximum Size of Startup-Config and Running-Config Files

Each ProCurve device has a maximum supported size for the running-config and the startup-config file. If you use TFTP to load additional information into a device’s running-config or startup-config file, it is possible to exceed the maximum supported size. If this occurs, you will not be able to save the configuration changes.

Table 7 lists the maximum size of the running-config and the startup-config files on ProCurve devices.

Table 7: Maximum Sizes Supported for running-config and the startup-config Files

Device	Maximum Size of running-config and startup-config files
ProCurve 9315 using Management II or higher	256 kilobytes (KB)
ProCurve 9304M or ProCurve 9308M using Management II or higher	256 KB
ProCurve 9304M or ProCurve 9308M using Management I (*discontinued*)	128 KB
ProCurve 6308M-SX or ProCurve 6208M-SX (*discontinued*)	64 KB

NOTE: The maximum supported file size of each file is not the combined size of the running-config and startup-config files. The running-config and startup-config files can each be the size listed in Table 7.

To determine the size of an ProCurve device’s running-config or startup-config file, copy the file to a TFTP server. Then use the directory services on the server to list the size of the copied file. To copy the running-config or startup-config file to a TFTP server, use one of the following commands.

- To copy the running-config to a TFTP server:

  copy running-config tftp <*ip-addr*> <*filename*>

- To copy the startup-config file to a TFTP server:

  copy startup-config tftp <*ip-addr*> <*filename*>

Removing a Module from an Active Device

Before you remove a module from a routing switch in operation, first disable the module. Disabling the module before removing it prevents a brief service interruption on other unmanaged modules. The brief interruption can be caused by the device re-initializing other modules when you remove an enabled module.

NOTE: This section does not apply to the active or standby Redundant Management modules. The **disable module** and **enable module** commands are not supported on management modules.

To disable a module, enter the following command at the Privileged EXEC level of the CLI:

disable module <*slot-num*>

Where <*slot-num*> specifies the slot number as follows:

- Slots in a 4-slot chassis are numbered 1 – 4, from top to bottom.
- Slots in an 8-slot chassis are numbered 1 – 8, from left to right.
- Slots in a 15-slot chassis are numbered 1 – 15, from left to right.

Example

```
ProCurve 9300# disable module 3
```

This command disables the module in slot 3.

NOTE: If you remove the module without first disabling it, the routing switch re-initializes the other modules in the device, causing a brief interruption in service after which the device resumes normal operation.

You do not have to enable a module after inserting it in the chassis. The module is automatically enabled when you insert the module into a running device or when you power on the device.

To replace a removed module with a different type of module, you must configure the slot for the new module. To configure a slot for a module, use the **module** command at the global CONFIG level of the CLI.

After disabling a module, if you decide not to remove the module, re-enable the module using the following command:

enable module <*slot-num*>

Example

The following command re-enables the module in slot 3:

```
ProCurve 9300# enable module 3
```

Configuring the ProCurve 9315M

When configuring a ProCurve 9315M 15-slot routing switch, take into account the guidelines and restrictions in this section.

Minimum Software Release Supported

The ProCurve 9315M requires software release 07.5.04 or greater.

NOTE: On a ProCurve 9315M, software release 07.5.04 is the earliest release supported. If a management module is running software earlier than release 07.5.04, you cannot upgrade the module in a 9315M chassis. Instead, you must upgrade it in a 9304M or 9308M chassis. For more information, see “Upgrading Software on an M2, M4, or EP Management Module to Release 07.8.01d” on page 7.

Inserting or Removing an EP Module on a ProCurve 9315M

NOTE: This section applies only to a ProCurve 9315M (15-slot chassis) with EP modules.

Do not insert or remove EP modules in a ProCurve 9315M until the device has fully booted. Generally, booting takes around two minutes. You can determine whether the device has fully booted by looking at the management console. Once the device boots, a command prompt or login prompt is displayed.

After the device has booted, allow time for the device to fully complete the removal or insertion before removing or inserting another module. Generally, this takes about 30 seconds. After you remove or insert a module, the CLI displays a message confirming completion of the change. Wait for this message before removing or inserting another module.

Slot Locations for Redundant Management Modules

The 15 slots in the ProCurve 9315M are divided among 4 internal regions. Slots 1 – 4 belong to the same region; slots 5 – 8 belong to the same region; slots 9 – 12 belong to the same region, and slots 13 – 15 belong to the same region. If you are using redundant management modules, ProCurve recommends that you place both management modules in slots belonging to the same region. For example, if you place one management module in slot 5, ProCurve recommends that you place the other management module in slot 6, 7, or 8.

MAC Addresses

The ProCurve 9315M makes use of locally administered MAC addresses. If your site already uses locally administered MAC addresses of the vendor OUI, which is 00e052, there could be a MAC address conflict with one of the ports on the ProCurve device.

Server Trunk Groups

If you plan to configure ports on a module into a server trunk group, use the following guideline:

- For a multi-slot trunk group (one configured on two forwarding modules), the modules must both be in the same set of slots (slots 1 – 7 or 9 – 15).

You do not need to follow this guideline for a switch trunk group.

NOTE: In software releases earlier than 07.6.00, the management module(s) and the module that had the server trunk group's ports were required to be in the same set of slots (slots 1 – 7 or 9 – 15). In software release 07.6.00 and later, there is no longer a restriction on the location of the management module relative to the module used for server trunking. However, it is still a requirement that the module that has the server trunk group's lead ports cannot reside in slot 8.

VLANs

In release 07.6.01b, you could configure only up to 2195 Layer 2 VLANs on the ProCurve 9315M routing switch. The **system-max vlan <num>** command allowed you to allocate a higher number of VLANs, but the software allowed you to actually create only 2195 of the allocated VLANs.

Starting with release 07.6.04, this restriction has been removed. You can create the full number of allocated Layer 2 VLANs on the 15-slot ProCurve 9315M routing switch, up to 4095.

These release notes describe new software enhancements in software release 07.8.01. See the following:

- "Summary of Enhancements in 07.8.01"
- "Software Fixes"

Summary of Enhancements in 07.8.01

Layer 3 Enhancements in 07.8.01

Enhancement	Description	EP	Non-EP	See Page
Configurable timers for RIP	The new **timers-basic** command allows you to set the RIP update timer, aging timeout interval, and garbage-collection timer.	✓	✓	17

Layer 2 Enhancements in 07.8.01

Enhancement	Description	EP	Non-EP	See Page
Private VLAN enhancements	In releases prior to 07.8.01, the private VLAN feature did not work properly when the ports in the private VLAN were configured as tagged. In this release, the VLAN ID is correctly replicated to the isolated VLAN.	✓	✓	17

System-Level Enhancements in 07.8.01

Enhancement	Description	EP	Non-EP	See Page
Specifying a minimum number of ports for a trunk group	You can configure the ProCurve device to disable all of the ports in a trunk group when the number of active member ports drops below a specified threshold value.	✓		18
CPU protection support	Release 07.8.01 supports the CPU protection feature. In addition, you no longer need to disable and re-enable the CPU protection feature when you add or remove a VLAN.	✓	✓	18
Hardware flooding enhancements	The commands **hardware-flooding**, **multicast-flooding**, and **broadcast-flooding**, which were available at the VLAN configuration level in previous releases, are no longer available in release 07.8.01. Instead of these commands, use the global **cpupro-action** command to activate CPU protection for all VLANs configured on the device. This new method improves upon the previous hardware flooding method in that you do not need to reload the software when a VLAN is added or deleted.	✓	✓	18

Enhancement	Description	EP	Non-EP	See Page
Dynamic ACL assignment for 802.1X multiple-host configurations	Starting with release 07.8.01, dynamic IP ACL and MAC address filter assignment is now supported in an 802.1X multiple-host configuration. If there are multiple hosts connected to a single 802.1X-enabled port, RADIUS-specified IP ACLs and MAC filters can be applied to each host, independent of the other hosts connected to the port.	✓	✓	19
New SNMP MIB table for MAC Port Security	The MAC Port Security table is the SNMP MIB equivalent of the **show port security mac** CLI command.	✓	✓	21
New trap message for port priority changes	A trap message is generated when a port's priority is changed.	✓	✓	22
New OIDs	The SNMP MIB OIDs for the snPortMonitorTable has been changed from "23" to "25".	✓	✓	23

Enhancements and Configuration Notes in 07.8.01d

Setting RIP Timers

In release 07.8.01d, you can set three new timers for the RIP protocol. The new **timers-basic** command allows you to set the RIP update timer, aging timeout interval, and garbage-collection timer. The RIP protocol must be enabled on the ProCurve device in order to set these timers.

The RIP **update-time** command, available in previous releases, has lower priority than the **timers-basic** command. If both commands are configured on the device, then the **update-time** command is ignored.

For example, the following command sets the three RIP timers:

```
ProCurve 9300(config) router rip
ProCurve 9300(config-rip-router)# timers-basic 5 15 15
```

Syntax: [no] timers-basic <update-timer> <aging-timeout-interval> <garbage-collection-timer>

The <update-timer> specifies how often RIP update messages are sent. You can specify from 1 – 1,000 seconds. The default is 30 seconds.

The <aging-timeout-interval> specifies how long the ProCurve device waits for a route update before declaring a route invalid. The value specified for the <aging-timeout-interval> should be at least three times the value specified for the <update-timer>. The <aging-timeout-interval> can be from 3 – 3,000 seconds. The default is 180 seconds.

The <garbage-collection-timer> specifies how long the ProCurve device waits for a route update before removing the route from the RIP route table. The value specified for the <garbage-collection-timer> should be at least three times the value specified for the <update-timer>. The <garbage-collection-timer> can be from 3 – 3,000 seconds. The default is 120 seconds.

Private VLAN Enhancements

In releases prior to 07.8.01d, the private VLAN feature did not work properly when the ports in the primary VLAN were configured as tagged. In this release, the VLAN ID is correctly replicated to the isolated VLAN, allowing support for tagged ports in the primary VLAN.

In addition, a primary VLAN can now have multiple promiscuous ports, allowing connections to multiple routers in the primary VLAN. In previous releases, when the primary VLAN consisted of more than one port, only the port with the lowest port number was promiscuous.

For information on configuring the private VLAN feature, see the *Installation and Basic Configuration Guide*.

Specifying a Minimum Number of Ports for a Trunk Group

In release 07.8.01d, you can configure the ProCurve device to disable all of the ports in a trunk group when the number of active member ports drops below a specified threshold value. For example, if a trunk group has 10 ports, and the threshold for the trunk group is 5, then the trunk group is disabled if the number of available ports in the trunk group drops below 5. If the trunk group is disabled, then traffic is forwarded over a different link or trunk group.

For example, the following commands establish a trunk group consisting of 4 ports, then establish a threshold for this trunk group of 3 ports.

```
ProCurve 9300(config)# trunk e 3/31 to 3/34
ProCurve 9300(config-trunk-3/31-3/34)# threshold 3
```

In this example, if the number of active ports drops below 3, then all the ports in the trunk group are disabled.

Syntax: [no] threshold <number>

You can specify a threshold from 1 (the default) up to the number of ports in the trunk group.

Notes:

- The **disable module** command can be used to disable the ports on a module. However, on 10 Gigabit modules, the **disable module** command does not cause the remote connection to be dropped. If a trunk group consists of 10 Gigabit ports, and you use the **disable module** command to disable ports in the trunk group, which then causes the number of active ports in the trunk group to drop below the threshold value, the trunk group is not disabled.
- If you establish a threshold for a trunk used in conjunction with the Metro Ring Protocol (MRP), then you must also enable Remote Fault Notification (RFN) for 1 Gigabit interfaces, or Link Fault Signalling (LFS) for 10 Gigabit interfaces.

CPU Protection Enhancement

Release 07.8.01d supports the CPU protection feature. For information on configuring this feature, see "Configuring CPU Protection" in the June 2005 or later edition of the *Security Guide*. In release 07.8.01d, the feature works as documented, but with the following enhancement:

In previous releases that supported CPU protection, you needed to disable and re-enable the feature whenever you added or removed a VLAN. Starting with release 07.8.01d, you enter the **cpupro-action hardware-flooding refresh** command when you add or remove a VLAN. This command refreshes the Layer 2 CAM used for hardware flooding. You no longer need to disable and re-enable CPU protection when you add or remove a VLAN.

For example, the following commands add a port to VLAN 111 and refresh the Layer 2 CAM used for hardware flooding:

```
ProCurve 9300(config)# vlan 111
ProCurve 9300(config-vlan-111)# untagged e 2/20
ProCurve 9300(config-vlan-111)# exit

ProCurve 9300(config)# cpupro-action hardware-flooding refresh
```

Syntax: [no] cpupro-action hardware-flooding refresh

Hardware Flooding Enhancements

The commands **hardware-flooding**, **multicast-flooding**, and **broadcast-flooding**, which were available at the VLAN configuration level in previous releases, are no longer available in release 07.8.01d. Instead of these commands, use the global **cpupro-action** command to activate CPU protection for all VLANs configured on the

device. This new method improves upon the previous hardware flooding method in that you do not need to reload the software when a VLAN is added or deleted. In addition, when configured, the new method applies globally to all VLANs, not just to individual VLANs.

For example, the following command enables hardware flooding for multicast traffic for all VLANs configured on the device:

```
ProCurve 9300(config)# cpupro-action hardware-flooding multicast-flooding on
```

To disable hardware flooding for multicast traffic for all VLANs configured on the device, enter the following command:

```
ProCurve 9300(config)# no cpupro-action hardware-flooding multicast-flooding on
```

Syntax: [no] cpupro-action hardware-flooding [multicast-flooding | broadcast-flooding | unknown-unicast-flooding] [on | off]

NOTE: Note that this new hardware flooding method works in conjunction with the CPU protection feature mentioned above. ProCurve recommends that you do not use the new hardware flooding method at the same time that you use the CPU protection feature.

Specifying the Toggle Time Interval for Unknown Unicast Traffic

When hardware flooding is enabled for unknown unicast traffic, some unknown unicast packets are periodically sent to the CPU so that CAM entries can be created for individual destinations.

You can configure how often unknown unicast traffic is sent to the CPU by specifying the ***toggle time interval*** for unknown unicast traffic. The device alternates between flooding unknown unicast traffic and sending it to the CPU according to the specified toggle time interval.

For example, if you specify a toggle time interval of 10 seconds, the device will alternately flood unknown unicast traffic for 10 seconds, then send unknown unicast traffic to the CPU for 10 seconds.

To specify a toggle time of 10 seconds on the ProCurve device, enter the following command:

```
ProCurve 9300(config)# cpupro-action unknown-unicast-toggle-time 10
```

Syntax: cpupro-action unknown-unicast-toggle-time <interval>

The <interval> can be from 1 – 60 seconds. The default is 5 seconds.

Dynamic ACL Assignment for 802.1X Multiple-Host Configurations

Starting in release 07.8.00, if there are multiple hosts connected to a single 802.1X-enabled port, the ProCurve device authenticates each of them individually. Each host's authentication status is independent of the others, so that if one authenticated host disconnects from the network, it has no effect on the authentication status of any of the other authenticated hosts.

In release 07.8.01d, dynamic IP ACL and MAC address filter assignment was not supported in an 802.1X multiple-host configuration, only for single host connected to the port. In an 802.1X multiple-host configuration, if a RADIUS server returned an Access-Accept message that specified an IP ACL or MAC address filter for the Client, these attributes were ignored.

Starting with release 07.8.01d, dynamic IP ACL and MAC address filter assignment is now supported in an 802.1X multiple-host configuration. If there are multiple hosts connected to a single 802.1X-enabled port, RADIUS-specified IP ACLs and MAC filters can be applied to each host, independent of the other hosts connected to the port.

Flow-Based IP ACLs

In releases prior to 07.8.00, IP ACLs that were dynamically assigned using a RADIUS server were ***rule-based***, meaning that when the IP ACL was assigned, entries were immediately programmed into CAM. Starting with release 07.8.01d, dynamically assigned IP ACLs are **flow-based**, meaning that entries are programmed into CAM after the flow is processed by the CPU. A flow is defined as traffic with a common source IP address, destination IP address, protocol, source port, and destination port.

When this feature is configured, any new flow received on an interface is sent to the CPU for processing. If there is an IP ACL to be applied to the flow, based on its 802.1x information (authentication status and MAC address), the CPU programs CAM entries to permit or deny the flow.

To use the flow-based ACL mechanism, you must enable flow-based ACLs on the 802.1X-enabled interfaces, and you must define a “placeholder” ACL to force a packet from each new flow to the CPU for processing. If you are using router code, and wish to filter traffic on a virtual routing interface (VE), you must enable traffic filtering on the VE. If you want to filter packets denied by ACLs in hardware, you must enable hardware filtering on the device.

Notes:

- Dynamically assigned outbound ACLs are supported in switch code only.
- Only one dynamically assigned MAC filter can be applied on a port at a time. This means that if an 802.1X-enabled port currently has a dynamically assigned MAC filter applied to it, and a host on the same port is subsequently authenticated, then any MAC filter information returned for the second host is ignored (although the second host is authenticated).

Configuring Dynamic ACL Assignment for an 802.1X Multiple-Host Configuration

To configure dynamic ACL assignment for an 802.1X multiple-host configuration, you perform the following tasks:

- Enable dynamic ACLs and MAC address filters for 802.1X multiple-host configurations on the ProCurve device
- Enable flow-based ACLs on the 802.1X-enabled interfaces
- Configure a “placeholder” ACL so that the initial packets of a flow are sent to the CPU for processing
- Enable traffic filtering on a virtual routing interface (if necessary)
- Enable hardware filtering of denied packets (if necessary)

Enabling Dynamic ACLs and MAC Address Filters for 802.1X Multiple-Host Configurations

To globally enable dynamically assigned IP ACLs and MAC address filters for 802.1X multiple-host configurations, enter the following commands:

```
ProCurve 9300#(config) dot1x enable
ProCurve 9300#(config-dot1x)# multi-user-policy enable
```

Syntax: [no] multi-user-policy enable

Enabling Flow-Based ACLs on the 802.1X Interfaces

Since the ACLs used in a 802.1X multiple-host configuration are flow-based, you must enable flow-based ACLs on the device. For example, to do this on interface 3/11, enter the following commands:

```
ProCurve 9300#(config) interface e 3/11
ProCurve 9300#(config-if-e1000-3/11)# ip access-group flow-mode
```

Syntax: [no] ip access-group flow-mode

Configuring a Placeholder ACL

Since the dynamically assigned ACLs used in 802.1X multiple-host configuration are flow-based, a packet from each new flow must be sent to the CPU for processing. If there is an IP ACL to be applied to the flow, based on its 802.1x information (authentication status and MAC address), the CPU then programs CAM entries to permit or deny the flow.

To cause the device to send the initial packet in a flow to the CPU, you create a “placeholder” ACL and apply it to the interface. This placeholder ACL should specify a host that does not exist in the network, so that the placeholder ACL does not affect traffic from a real host.

For example, the following commands create an ACL that filters TCP, UDP and/or ICMP traffic and then apply the ACL to inbound and outbound traffic on an interface:

```
ProCurve 9300(config)# access-list 131 deny tcp host 1.1.1.1 any
ProCurve 9300(config)# access-list 131 deny udp host 1.1.1.1 any
ProCurve 9300(config)# access-list 131 deny icmp host 1.1.1.1 any
ProCurve 9300(config)# access-list 131 permit ip any any
```

```
ProCurve 9300(config) interface e 3/11
ProCurve 9300#(config-if-e1000-3/11)# ip access-group flow-mode
ProCurve 9300#(config-if-e1000-3/11)# ip access-group 131 in
ProCurve 9300#(config-if-e1000-3/11)# ip access-group 131 out
ProCurve 9300#(config-if-e1000-3/11)# exit
```

When the placeholder ACL is applied, any new IP traffic flow on interface 3/11 is directed to the CPU. If the source MAC address of the flow is already associated with a successfully authenticated 802.1X host that has a dynamically assigned IP ACL applied to it, then that dynamically assigned IP ACL is applied to the flow. Note that if there is a user-defined ACL for this MAC address, the placeholder ACL is ignored, and only the user-defined ACL is applied to the flow.

Filtering Traffic on a Virtual Routing Interface (VE)

If the ACL is to process traffic on a virtual routing interface (VE), you must enable traffic filtering on the VE.

By default, the ProCurve device does not filter traffic that is switched from one port to another within the same VE, even if an ACL is applied to the interface. You can enable the device to filter switched traffic within a virtual routing interface. When you enable the filtering, the device uses the ACLs applied to inbound traffic to filter traffic received by a port from another port in the same virtual routing interface. This feature does not apply to ACLs applied to outbound traffic.

For example, the following commands enable traffic filtering on VE 1:

```
ProCurve 9300(config)# int ve 1
ProCurve 9300(config-vif-1)# ip access-group ve-traffic
```

Syntax: [no] ip access-group ve-traffic

Enabling Hardware Filtering of Denied Packets

To configure the device to filter denied packets in hardware, rather than using the CPU, enter the following command:

```
ProCurve 9300(config)# hw-drop-acl-denied-packet
```

Syntax: [no] hw-drop-acl-denied-packet

When you enable hardware filtering of denied packets, the CPU creates a CAM entry for the denied packet. Subsequent packets with the same address information are filtered using the CAM entry. The CAM entry ages out after two minutes if not used.

New SNMP MIB Table for MAC Port Security

The new SNMP MAC Port Security table shows the same information as the **show port security mac** CLI command.

Name, Identifier, and Syntax	Access	Description
snPortMacSecurityTable 1.3.6.1.4.1.1991.1.1.3.24.1.1.1	N/A	The MAC Port Security table.
snPortMacSecurityEntry 1.3.6.1.4.1.1991.1.1.3.24.1.1.1.1	N/A	An entry in the MAC Port Security table.
snPortMacSecurityIfIndex 1.3.6.1.4.1.1991.1.1.3.24.1.1.1.1.1 Syntax: Unsigned32	Read only	The ifIndex value (ID) of the Ethernet interface on which MAC port security is enabled.

snPortMacSecurityResource 1.3.6.1.4.1.1991.1.1.3.24.1.1.1.1.2 Syntax: Integer	Read only	Indicates how the MAC addresses on an interface are secured: local(1) – Local resource was used. The interface secures at least one secure MAC address entry. Each interface can store up to 64 local resources. shared(2) – Shared resource was used. When an interface has secured enough MAC addresses to reach its limit for local resources, it can secure additional MAC addresses by using global or shared resources.
snPortMacSecurityQueryIndex 1.3.6.1.4.1.1991.1.1.3.24.1.1.1.1.3 Syntax: Unsigned32	Read only	An index for a MAC address entry that was secured for this interface.
snPortMacSecurityMAC 1.3.6.1.4.1.1991.1.1.3.24.1.1.1.1.4 Syntax: Integer	Read only	The secured MAC address.
snPortMacSecurityAgeLeft 1.3.6.1.4.1.1991.1.1.3.24.1.1.1.1.5 Syntax: Unsigned32	Read only	The number of minutes the MAC address will remain secure.
snPortMacSecurityShutdownStatus 1.3.6.1.4.1.1991.1.1.3.24.1.1.1.1.6 Syntax: Integer	Read only	Indicates if the interface has been shut down due to a security violation. up(1) – The port is up. down(2) – The port has been shut down.
snPortMacSecurityShutdownTimeLeft 1.3.6.1.4.1.1991.1.1.3.24.1.1.1.1.7 Syntax: Unsigned32	Read only	If the value of the snPortMacSecurityShutdownStatus is down(2), this object shows the number of seconds before it is enabled again. If the value is up (1), this object shows 0.
snPortMacSecurityVlanId 1.3.6.1.4.1.1991.1.1.3.24.1.1.1.1.8 Syntax: Unsigned32	Read only	Shows the VLAN membership of this interface. This object shows a value from 1 – 65535.

New Trap Message

Trap Name and Number	Varbinds	Severity	Description and Trap Message
snTrapPortPriorityChange(122)	snAgGblTrapMessage	Informational	This trap is generated when a port's priority is changed. **Format:** Port <port-number> priority changed to <new-priority>

Changes to snPortMonitor OID

The object identifiers (OIDs) for the snPortMonitorTable has been changed from “23” to “25”. The following objects have new OIDs:

- snPortMonitorTable – 1.3.6.1.4.1.1991.1.1.3.25.1
- snPortMonitorEntry – 1.3.6.1.4.1.1991.1.1.3.25.1.1
- snPortMonitorIfIndex – 1.3.6.1.4.1.1991.1.1.3.25.1.1.1
- snPortMonitorMirrorList – 1.3.6.1.4.1.1991.1.1.3.25.1.1.2

Software Fixes

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
	07.8.01			
14668	Although rare in occurrence, In some configurations with EBGP, IBGP, and OSPF routes, the ProCurve device may not always select the best route. For example, the device might install an IBGP route in the routing table, even though the IBGP route has a higher administrative distance than OSPF. This could happen if the device previously selected an EBGP route as the best route. If this problem occurs, you must clear the routing table, after which the ProCurve device will select the best route.	BGP		07.8.01

25042	Module: 8-port Gigabit Management Module
	If you configure a port name on the primary port of a trunk group, the software generates an error message when the device boots up. For example, the following configuration generates an error at boot-up:
	`ProCurve(config)#int e 1/3`
	`ProCurve(config-if-e1000-1/3)#port-name “testtrunk”`
	However, if you configure a port name on all of the members of the trunk group, this error does not occur. For example:
	`ProCurve(config)#trunk switch e 1/3 to 1/4`
	`ProCurve(config-trunk-1/3-1/4)#port-name “testtrunk”`
		CLI		07.8.01

25049, 25455	A port operating at **10-half** (10 Mbps at half duplex) drops 80% of broadcast traffic to other ports in the VLAN. This does not occur if the port is configured to operate at 100-full.	IP Stack		07.8.01

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
29177	Module: 8-port mini-GBIC M4 Management Module A deny clause in an outbound ACL does not work if the destination IP address has been aggregated using the **IP net aggregate** command.	ACL		07.8.01
29465	Module: Standard 24-port 10/100 Module MRP disables 10/100 copper MRP ring interfaces that are set to **100-full** speed and duplex mode. In addition, the output of the **show interface brief** command shows that the interfaces are “blocked”.	24-port 10/100 Module		07.8.01
29469	The **peer MAC address or IP** field for the VSRP standby displays “unknown” even if the VSRP standby knows the IP address of the master router.	VSRP		07.8.01
29670	If you enable 802.1W (**spanning-tree** command) on a port-based VLAN before configuring the port as tagged or untagged, 802.1W fails to initialize. As well, the **show 802-1w** command output shows that RSTP is not configured. Note that if you define the port as tagged or untagged before enabling 802.1W, this problem does not occur.	RSTP - IEEE 802.1w		07.8.01
29755	The following display message contains a typo: `mtu config change detected, if NOT hot swaping, please save and reload!` This message should read “swapping” instead of “swaping”.	Jumbo IP Packet Support		07.8.01
29759	If jumbo packets (**default-mtu 14336** command) are enabled globally on the ProCurve device and the device has an empty module slot or slots, the ports on the empty module slots are configured with **mtu 1518** instead of **mtu 14336**. This occurs after issuing the **write memory** command.	Jumbo IP Packet Support		07.8.01
29846	If you hot-insert a module in a ProCurve device that is globally configured to support jumbo frames (**default-mtu 14336** command), the newly installed module should automatically inherit the jumbo configuration without requiring a software reload. However, this does not occur and jumbo frame support is not recognized on the newly installed module unless you reload the software.	Jumbo IP Packet Support		07.8.01
30248	If the ProCurve device has numerous BGP entries, the page break (page display) does not work properly with the **show ip bgp peer** command. After entering the **show ip bgp peer** command, the command output scrolls continuously on the screen at first, then goes into page-by-page prompting mode.	BGP		07.8.01

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
30685	The ProCurve device deletes a route from the routing table even though the same entry exists in the LSA database.	OSPF		07.8.01
30702	The **no ip ospf cost <cost value>** command does not apply the default value to the cost.	OSPF		07.8.01
30998	The ProCurve device prefers OSPF routes over EBGP routes after a software reload. If you clear BGP sessions or IP routes, this problem does not occur.	BGP		07.8.01
31047	If the ProCurve device has one BGP neighbor, the software increases the ARP timer and eventually ages out the ARP entry for the peer. This error does not occur if there are two BGP neighbors. In this case, the ARP timers stay between 0 and 1.	BGP4+		07.8.01
31084	Module: 8-port mini-GBIC M4 Management Module The ProCurve device reloads the software after receiving an invalid header length value in BGP packets.	BGP4+		07.8.01
31157	A BGP router fails to send notification after clearing a peer session.	BGP4+		07.8.01
31166	OSPF fails to delete a redistributed static route from the routing table even though the static route has been removed.	OSPF		07.8.01
31543	Module: 8-port mini-GBIC Management Module Although rare in occurrence, a software reload can occur in configurations with OSPF, when Remote Fault Notification (RFN) is enabled or disabled on a Gigabit Ethernet fiber port.	OSPF		07.8.01
31649	Module: 8-port mini-GBIC Management Module If an active management module fails over to the standby management module, the standby management module does not inherit the jumbo frame configuration from the active management module.	Jumbo IP Packet Support		07.8.01
31734	The ProCurve device reloads the software if the configuration includes Internet Group Management Protocol (IGMP) snooping and the hash table has a NULL value.	Other		07.8.01
31925	The copper mini-GBICs can operate in 1000 Mbps autonegotiation mode only. You cannot configure them to operate in other modes. However, if you insert a mini-GBIC (M-TX) into an LX or SX port, the CLI allows you to configure the mini-GBIC to a speed other than 1000 Mbps.	CLI		07.8.01

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
32021	The ProCurve device does not decrement the TTL when a VSRP packet passes through it.	VSRP		07.8.01
32192	VRRP-E link state flapping (fluctuating between up and down), causes the device to reload the software. This occurs on a device with a non-T-Flow management module.	Other		07.8.01
32230	Module: 8-port mini-GBIC M4 Management Module When the ProCurve device uses an ACL TCP established clause, an ACL incorrectly permits a series of SYN packets after it receives an ACK packet with a TTL of 0 (zero).	ACL		07.8.01
32360	Module: EP10/100 RJ-45 module. The ProCurve device does not successfully remove some ACL remarks and line entries from the configuration. This occurs if you delete an ACL (for example, **no access-list 130**) then later create an ACL with the same ACL number (for example, **access-list 130**). In this case, the software incorrectly inserts some of the remarks and entries from the previously deleted ACL.	ACL		07.8.01
32448	Module: 8-port mini-GBIC M4 Management Module The ProCurve device sends PIM registration packets with the wrong source IP address.	PIM Sparse		07.8.01
32462	The **show debug** command output does not indicate that any of the debug span or debug 802.1w commands have been enabled on the ProCurve device.	CLI		07.8.01
32735	The ProCurve device corrupts the Autonomous System (AS) path if all three of the following conditions exist: • The ProCurve device is configured to remove private AS numbers from update messages sent to a neighboring device (**remove-private-as** command). • The ProCurve device is configured to aggregate AS-path information for all the routes in the aggregate (**as-set** parameter). The first **as-set** segment has a private AS number.	BGP		07.8.01
32854	Module: EP 48-port RJ-45 module A port's Full Duplex (FDX) LED does not illuminate even though the port has a fixed configuration of 100 full-duplex, and the port is connected to another ProCurve device that also has a fixed 100 full-duplex configuration.	10/100 MAC		07.8.01

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
32857	Connectivity issues may occur If MAC authentication is enabled on an IronCore device.	MAC Authorization		07.8.01
32906	The software truncates the number of days timestamp for buffered Syslog messages. For example, if the actual system uptime is: 382 days 23 hours 17 minutes 26 seconds the software displays: 38 days 23 hours 17 minutes 26 seconds	Syslog		07.8.01
33511	The ProCurve device incorrectly load balances traffic across the ports in a trunk group, if a port in the trunk group goes down then comes up again. In this case, the device should re-balance the traffic so that all of the ports in the trunk group are properly utilized.	Other		07.8.01
33834	The software incorrectly attempts to free a TCB block that was already previously released. This causes the device to display a warning message on the console.	TCP Stack		07.8.01
34493	If an ACL statement contains a range of values, the ACL **log** option, **dscp-marking**, and other ACL options may not be available in the CLI. For example, if you create an ACL entry that denies a TCP port range (e.g., **access-list 1 deny tcp any any range 127 129**), some ACL options that are normally available immediately following this command, are not available at all.	ACL		07.8.01
34507	In an MRP configuration with four devices in a ring and two rings in two different VLANs (for example, one ring in VLAN 10 and another ring in VLAN 30), an MRP ring fails to come up after a reboot.	MRP		07.8.01
	07.8.01a			
34160	Routing stops to the monitor port when mirror/ monitoring is enabled. Duplicate of 40149.	Mirror/ Monitoring		07.8.01a
35710	The command “no web management” disables access on port 80, but access on port 280 is permitted.	Web Management		07.8.01a
37911	Radius-server <hostname> re-orders parameters incorrectly.	RADIUS		07.8.01a
40619	Crypto random gen command is incomplete	Encryption		07.8.01a
43703	Access is granted without password verification.	Password		07.8.01a

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
	07.8.01b			
31957	Error: “w_mtu_buffer_type_config_write() to standby management jumbo e2 prom error” when using a “wr mem” command via a telnet session.	CLI	07.8.00	07.8.01b
33508	CPU will go up when a “sh tech” is issued via a SSH session. As a result, VRRP failovers and some 802.1w transitions may occur.	VRRP-E, RSTP, 802.1w	07.6.06	07.8.01b
34609	10G link stays up when the egress side of the link is disabled. No LFS configured.	10G link	07.6.06	07.8.01b
35199	Switch crash with Data Access Exception in “sw_12_get_outgoing_port_by_da_match” while forwarding sFlow packets due to invalid port number on r29.	sFlow	07.6.06	07.8.01b
36363	Error: “WARN: Out of timer entry” appears repeatedly after adding VLAN group with large number of VLANs or after reloading.	VLAN	07.8.01	07.8.01b
41689	The show pid being displayed as part of the “show tech” command will cause a brief cpu utilization spike.	CPU	07.6.06	07.8.01b
43660	Switch Data Access Exception crash in “ssh-vsnprintf_internal” if SSH key is generated using the “crypto key generate rsa” command.	SSHv2	07.8.01	07.8.01b
43861	Router may reload with Program Exception in “ssh_private_key_derive_public_key” when enabling SSH.	SSh	07.8.00	07.8.01b
44042	Reload may occur when SSH into a switch with a crash dump including “ssh_server_destroy”.	SSH	07.8.00	07.8.01b
44364	The OSPF neighbor fails to come up because of authentication key failure.	OSPF	07.6.06	07.8.01b
45071	Error messages and stuck CAM are displayed after deleting ACL “access-list 100 deny ip 0.0.0.0 0.255.255.255 any”.	ACL, CAM	07.6.06	07.8.01b
45198	Port 280 stays open if you enter “no web-management http” followed by “no web-management hp-top-tools.”	Web Mgmt	07.8.01	07.8.01b
45319	Error: “Exceed max DMA 9 L4 cam resource, using flow-based ACL instead” message is displayed in the log when running the “ip rebinding acl all” command.	ACL	07.8.00	07.8.01b
46742	Web access group router ACL does not send RST until after the TCP 3-way handshake completes.	ACL	07.8.01	07.8.01b

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
46777	The global setting for sFlow sampling rate is not applied to secondary trunk links on startup when config-trunk-ind is used.	sFlow	07.6.06	07.8.01b
46924	The command “sFlow sample <x>” at the trunk level does not work upon reload.	sFlow	07.6.06	07.8.01b
47724	The command “sh ip bgp nei <x> adv” may not show all the advertised routes - display issue only.	CLI	07.8.00	07.8.01b
47855	Continuous error: “OSPF TIMER: Warning Checksum bad in Link State Database!”	OSPF	07.8.00	07.8.01b
48823	If you configure multiple addresses on an interface and reload, RIPv2 advertises from only the lowest IP address.	RIPv2	07.8.00	07.8.01b
49395	With trunk switch in L3 environment, if one of the trunk ports goes down and comes up again, outgoing traffic is not redistributed correctly on the member ports of the trunk group.	Trunk Group	07.6.06	07.8.01b
49672	Router crash in “12ka-pre_process_port_event” if a high numeric port number is configured.	System	07.8.01	07.8.01b
49695	OSPF send LS update with age=3600 while route map changed.	OSPF	07.6.06	07.8.01b
49914	When the router id is changed (modified IP address on loopback), OSPF stops advertising the default route.	OSPF	07.8.01	07.8.01b
	07.8.01c			
22489	When the primary link-aggregation (802.3ad) LACP port is disconnected, the secondary port goes into stp “disabled” state.	LACP	07.6.04	07.8.01c
33503	BGP routes are preferred over OSPF route after the BGP routes are withdrawn.	BGP, OSPF	07.8.00	07.8.01c
33598	Switch responding to SNMP get requests sent to destination IP addresses X.X.X. X. and MAC FFFF.FFFF.FFFF.	SNMp	07.8.00	07.8.01c
35968	Web server not functional, and exhibits XSS Vulnerability after running NeWT (Nessus Windows Technology).	Web Mgmt	07.8.00	07.8.01c
40784	When trying to generate a new RSA key, get error: “RSA key cannot be generated now, please try later” message.	RSA	07.6.05	07.8.01c
43721	Execution of the command “dm del <mod_slot#>” after insertion of 2-port 1-G module, causes router to reload.	10G	07.6.05	07.8.01c

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
44138	CPU spikes for about 8 seconds when adding or removing ports to a VLAN with outbound ACL configured.	CPU, ACL	07.6.06	07.8.01c
45057	The command “show cpu” shows 1% CPU utilization even though there are a very large number of packets going through the CPU.	CPU	07.8.00	07.8.01c
47395	If the primary link in an LACP 802.3ad trunk goes down for more than 90 seconds, then comes back up, port flapping occurs.	LACP	07.8.00	07.8.01c
47584	Possible Data Access Exception in “ipc_r_read” routine while adding MAC in a trunk group.	Trunk	07.6.06	07.8.01c
47825	RIP redistribution does not update the OSPF forwarding address field when RIP is updated.	RIP, OSPF	07.6.06	07.8.01c
48859	BGP router A redistributes tagged BGP route as OSPF LSA to router B running OSPF. Router B sends OSPF LSA to router C. If the BGP router A changes the tag, router C’s OSPF database is updated, but not the OSPF route.	BGP, OSPF	07.6.06	07.8.01c
49240	With a large number of modules in the 9315 chassis, if a 1g port is disconnected, you may see packet loss across a 10G link for 3-5 seconds.	10G	07.6.04	07.8.01c
49319	OSPF cannot add route from LS database due to no ip forward route.	OSPF	07.6.00	07.8.01c
49731	The trunk threshold command does not take effect until after a reload of the router. Also, when you remove a trunk and re-create a new trunk, the existing threshold value gets applied to the newly created trunk.	Trunk group	07.8.1	07.8.01c
49914	When you change the router id (modifying the ip address of loopback) OSPF stops advertising the default route. The problem is not seen if you always configure default-information-originate.	OSPF	07.8.00	07.8.01c
50203	Routing switch does not flash MAC address when MRP topology changes, even if the routing switch receives topology change packet.	MRP	07.8.00	07.8.01c
50541	Network latency jumps from sub millisecond to 300+ milliseconds when MAC filters are applied.	MAC filters	07.8.01	07.8.01c
50592	Multicast Jumbos does not work over 10G module.	Multicast	all	07.8.01c
51482	The system reloads when the command “ip tftp source loopback 19899960” is entered in the config mode. This is because the Valid Port Range is not checked.	CLI	07.8.00	07.8.01c

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
	07.8.01d			
34400	sFlow not picking up IP router-id or any physical address other than default. If sFlow running at time the address is changed, “sh sflow” reflects the new agent address, but trace shows new address is not being used (uses the default address).	sFlow	07.8.00	07.8.01d
44260	Accessing HTTP may cause the system to reload at “ProcessCookie”.	HTTP	07.8.01	07.8.01d
45319	Keep getting error: “Exceed max DMA 9 L4 cam resource, using flow based ACL instead” while issuing the command to “ip rebind-acl all”.	ACL	07.6.06	07.8.01d
47254	On a tagged port, wrong ACl is being applied to packets	ACL	07.8.00	07.8.01d
51175	Route fails to boot up properly when “sflow enable” is configured globally and “management-ip-disable” is configured on a ve.	sFlow	07.8.00	07.8.01d
51482	The system crashes at “ip_get_port_ip_address” when the “ip tftp source loopback 19899960” is configured, because the Valid Port Range is not checked.	CLI	07.8.00	07.8.01d
52419	SSH disconnects the SSH client after the Idle Time expires even with active CLI activity from this session.	SSH	07.8.00	07.8.01d
52659	IGMP query (to 224.0.0.1) goes through blocking port. This happens only when some port of this VLAN is a non-querier, or with different IGMP versions.	IGMP	07.8.01	07.8.01d
53881	SNMP OID “snAgentConfigModule” type displays the incorrect type for certain modules.	SNMP Mgmt	07.8.00	07.8.01d
54208	Unable to configure TFTP or telnet source-interface.	CLI	07.8.01	07.8.01d
54250	CLI command “debug span all_802_1D_events vlan <VID>” is not recognized even though it’s listed as an option.	802.1d, CLI	07.8.00	07.8.01d
54251	The command “debug 802.1w all_802_1W_events vlan” does not send any output to the console, telnet, or ssh sessions.	802.1d, CLI	07.8.00	07.8.01d
54375	Data Access Exception crash when the command “no unt eth 21 eth 22 eth 23 eth 24” command was executed after “qos-tos trust DSCP” had been configured.	DSCP, QOS	07.8.00	07.8.01d
54527	The command “debug ip ssh” gives “level 0” as an option.	CLI, SSH	07.8.00	07.8.01d

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
54542	Deleting a Group-vlan using the “no topology-group 1” or “no vlan-group 1...” to delete the virtual group-router-interface, does not delete the route from the route table.	CLI	07.8.00	07.8.01d
54572	Device reloaded with “TRAP REASON - External Interrupt” during SSH connection attempt.	SSH	07.8.01	07.8.01d
55039	OSPF age in the LS update or Data description packet may get corrupted. OSPF LSA age is 19218 on both routers. This causes them to send LSA updates to each other every second and these LSAs cannot be aged out.	OSPF	07.8.01	07.8.01d
55290	The command “de buffers” command causes display buffer leak, show command displays “INFO: all 11 display buffers are busy”.	CLI	07.8.00	07.8.01d

Known Issues in 07.8.01

This section lists the known issues in software release 07.8.01.

Table 8: Known Software Issues in Release 07.8.01

Bug ID	Bug Description	Protocol Feature
32126	An MSDP peer does not recover after a physical link that is a member of the MSDP peer goes down and recovers. Also, even though the physical links on both ends of the MSDP peer is down, one of the MSDP peer routers remains in an “established” state for three minutes before it transitions to an “Idle” state. Workaround: After the MSDP peer physical link recovers, clear the MSDP peer to establish a TCP connection (**clear ip msdp peer** command).	MSDP

ProCurve 9300M Series Modules

Table 9 lists the modules that are currently available for use in ProCurve 9300M Series routing switches. (Discontinued modules are also listed.)

Table 9: ProCurve 9300M Series Modules

Module Type	Part Number and Description	Module String
EP Redundant Management Modules	**J4885A** ProCurve 9300 EP 8-Port Mini-GBIC Redundant Management Module	EP-8-port-mini-GBIC-management

Module Type	Part Number and Description	Module String
EP Non-Management Modules	**J4881B** ProCurve 9300 EP 48-Port 10/100-TX RJ-45 Module	EP-48-port-10/100-TX-RJ45-module
	J4889B ProCurve 9300 EP 48-Port 10/100-TX Telco (RJ-21) Module	EP-48-port-10/100-TX-telco-module
	J4894A ProCurve 9300 EP 16-Port Mini-GBIC Module	EP-16-port-mini-GBIC-module
	J4895A ProCurve 9300 EP 16-Port 100/1000-T Module	EP-16-port-100/1000-T-module
	J8178A ProCurve 9300 EP 24-Port 100Base-FX Module	EP 24 Port 100Base-FX Module
Redundant Management modules (M2 and M4)	**J4845A** ProCurve 9300 GigLX Redundant Management Module (8-port)	8-port-gig-management-module Discontinued
	J4846A ProCurve 9300 GigSX Redundant Management Module (8-port)	8-port-gig-management-module Discontinued
	J4847A ProCurve 9300 Redundant Management Module (0-port)	0-port-management-module Discontinued
	J4857A ProCurve 9300 Mini-GBIC Redundant Management Module (8-port)	8-port-gig-m4-management-module Discontinued
	J4879A ProCurve 9300 T-Flow Redundant Management Module (0-port)	— Discontinued
Management modules (M1) Supported only on the ProCurve 9304M and ProCurve 9308M. (M1 modules are not supported on the ProCurve 9315M.)	**J4141A** ProCurve 9300 10/100 Management Module (16-port)	16-port-copper-management-module Discontinued
	J4144A ProCurve 9300 Gigabit SX Management Module (8-port)	8-port-gig-management-module Discontinued
	J4146A ProCurve 9300 Gigabit 4LX/4SX Management Module (8-port)	8-port-gig-management-module Discontinued

Module Type	Part Number and Description	Module String
Unmanaged Modules (Standard, non-EP)	**J4140A** ProCurve 9300 10/100 Module (24-port)	24-port-copper-module Discontinued
	J4142A ProCurve 9300 100Base FX Module (24-port MT-RJ)	24-port-100fx-module Discontinued
	J4143A ProCurve 9300 Gigabit SX Module (8-port)	8-port-gig-module Discontinued
	J4145A ProCurve 9300 Gigabit 4LX/4SX Module (8-port)	8-port-gig-module Discontinued
	J4842A ProCurve 9300 1000Base-T Module (8-port)	8-port-gig-copper-module Discontinued
	J4844A ProCurve 9300 GigLX Module (8-port)	8-port-gig-module Discontinued
	J4856A ProCurve 9300 Mini-GBIC Module (8-port)	8-port-gig-module Discontinued
10 Gigabit Ethernet Modules (Unmanaged, supported with both Standard and EP Management Modules)	**J4891A** ProCurve 9300 1-port 10 Gb Module	1-port-10Gig-module Discontinued
	J8174A ProCurve 9300 2-port 10 Gb Module	2-port-10Gig-module

—This page intentionally left blank—

5991-4722
March 2006